

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

**On Appeal to the Board of
Appeals and Interferences**

Appellant(s) : Ezawa et al. Examiner: Aravind K. Moorthy
Serial No. : 09/628,315 Group Art Unit: 2131
Filed : July 28, 2000
Title : SYSTEM AND METHOD FOR COMMUNICATING BETWEEN
SMART CARDS

AMENDED APPEAL BRIEF

I hereby certify that this paper is being electronically filed with the United States Patent and Trademark Office.

April 21, 2009

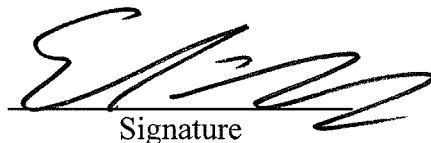
Date of Deposit

Eliot D. Williams

Attorney Name

50,822

Registration No.


Signature

April 21, 2009
Date of Signature

TABLE OF CONTENTS

| | | |
|-------|--|----|
| I. | REAL PARTY IN INTEREST | 3 |
| II. | RELATED APPEALS AND INTERFERENCES..... | 4 |
| III. | STATUS OF CLAIMS | 5 |
| IV. | STATUS OF AMENDMENTS | 6 |
| V. | SUMMARY OF CLAIMED SUBJECT MATTER | 7 |
| VI. | GROUND FOR REJECTION TO BE REVIEWED ON APPEAL..... | 12 |
| VII. | ARGUMENT..... | 13 |
| | A. The 35 U.S.C. § 112 First Paragraph Rejection Of Claims 25-58 Should Be Reversed | 13 |
| | B. The Rejections Under 35 U.S.C. § 102(b) based on Cucinotta Should be Reversed..... | 14 |
| | 1. Relevant Case Law | 14 |
| | 2. Ishiguro Does Not Disclose “If Device” | 15 |
| | C. The 35 U.S.C. § 103(a) Rejections Based On Ishiguro in view of Carlisle Should Be Reversed..... | 17 |
| | 1. Relevant Case Law | 17 |
| | 2. Ishiguro Does Not Disclose “If Device” and Carlisle fails to overcome this deficiency of Ishiguro..... | 18 |
| | D. Conclusion | 18 |
| VIII. | CLAIMS APPENDIX..... | 19 |
| IX. | EVIDENCE APPENDIX..... | 28 |
| X. | RELATED PROCEEDINGS APPENDIX | 29 |

TABLE OF AUTHORITIES

CASES

| | |
|--|----|
| <i>Graham v. John Deere</i> 383 U.S. 1 (1966) | 17 |
| <i>In re Bond</i> , 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990) | 15 |
| <i>In re Saunders</i> , F.2d 599, 602-03, 170 U.S.P.Q. 213, 444 (C.C.P.A. 1971) | 14 |
| <i>KSR Int'l Co. v. Teleflex Inc</i> 550 U.S. 398 (2007)..... | 17 |
| <i>Minnesota Mining and Manufacturing Co. v. Johnson & Johnson Orthopedics, Inc.</i> , 976 F.2d 1559, 24 U.S.P.Q.2d 1321 (Fed. Cir. 1985) | 14 |
| <i>Richardson v. Suzuki Motor Co.</i> , 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) | 14 |
| <i>Verdegaal Bros. v. Union Oil Co. of California</i> , 814 F.2d 628, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987) | 14 |

STATUTES

| | |
|--------------------------|----|
| 35 U.S.C. § 102(b) | 14 |
|--------------------------|----|

Commissioner for Patents
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Amended Appeal Brief is submitted in response to the Order Returning Undocketed Appeal to the Examiner from BPAI (hereafter "Order"), dated May 15, 2008 and further to the Examiner's phone call of March 27, 2009. The Order also alleges that "on page 2 of the Examiner's Answer, under the heading 'Summary of Claimed Subject Matter' the Examiner stated that 'The Summary of claimed subject matter contained in the brief is deficient...'" and that "...there is no indication that the Appellants responded to the Examiner's Answer." (Order, page 2). The Order also alleges that "[a] clarification of the claims to be applied in the rejection

is required.” (Order, page 2). Applicants submit the attached Amended Appeal brief to address the issues raised in the Order and during the Examiner’s phone call of March 27, 2009.

Appellant hereby files concurrent with this paper, an Amendment After Final Office Action, canceling claims 1-24.

I. REAL PARTY IN INTEREST

The real party in interest is MasterCard International Incorporated, 2000 Purchase Street, Purchase, New York 10577-2509 ("MasterCard") by virtue of purchase agreement with MONDEX INTERNATIONAL LIMITED assignee of the entire right, title, and interest in the present application by virtue of the Assignment dated July 25, July 26 and July 27, 2000, which was recorded on October 2, 2000 at Reel 1140 Frame 0006.

II. RELATED APPEALS AND INTERFERENCES

Appellants and the Appellants' legal representatives are unaware of any appeals or interferences related to the present application, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-58 stand rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement.

Claims 1-44 and 46-58 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Ishiguro et al. U.S. Patent No. 5,502,765 (“Ishiguro”). Claims 4 and 45 stand rejected under 35 U.S.C. § 103(a) as being obvious form Ishiguro in view of Carlisle et al. U.S. Patent No. 5,649,118 (“Carlisle”).

Claims 1-24 are concurrently cancelled, without prejudice. Claims 25-58 are now on appeal. A copy of all claims is attached hereto in the Claims Appendix at page 19.

IV. STATUS OF AMENDMENTS

Subsequent to the issuance of the Final Office Action, and in order to place this application in better condition for appeal and allowance, Appellant files and Amendment After Final concurrently herewith in accordance with 37 C.F.R. 41.33 to cancel claims 1-24.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Appellants' invention provides systems and methods for direct but secure transactions between smart cards (or other portable devices) without the need for accessing a host system to verify or authenticate process parameters such as time. According to applicants' invention, each smart card is embedded with its own trusted time clock, reference or parameter. (See e.g., specification page 5, lines 14-20). The embedded trusted time parameter may be hashed or otherwise represented by a sequence of numbers.

Independent claims 25, 32, 37, 41, and 54 are directed to the inventive systems and methods. All of these independent claims 25, 32, 37, 41, and 54 require key-secured communication between two smart cards to mutually update information based upon a comparison of trusted times that are embedded in each of the two smart cards. (See e.g., specification, page 18, lines 19-26.)

Written support for independent claims 25, 32, 37, 41, and 54 may be found in the specification as indicated below:

25. A portable device which is capable of performing a transaction with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device ; and [See e.g., Figure 2, specification, page 18, lines 1-3].

a processing device performing the following steps:

receiving a second sequence number and a second key from the further portable device, wherein the second sequence number comprises information on a second trusted time embedded in the further portable device[See e.g., specification, page 19, lines 4-10],

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times[*See e.g., specification, page 19, lines 4-10;*

performing a verification using the first and second keys [*See, e.g., specification, page 19, lines 10-11*];

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds[*See e.g., specification, page 18, lines 19-26, page 19, lines 20-25*]; and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device[*See e.g., specification, page 18, lines 19-26, page 19, lines 20-25*].

32. A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number, the second storage device storing thereon a second sequence number, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices [*See, e.g., Figure 2, specification, page 18, lines 1-3*], the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the first portable device, the second sequence number being indicative of the second trusted time provided on the second portable device[*See, e.g., specification, page 18, lines 1-3 and lines 10-18*]; and

if the first trusted time is older than the second trusted time, setting the first sequence number to have a value of the second sequence number [*See e.g., specification, page 18, lines 19-26*] and conversely,

if the second trusted time is older than the first trusted time, setting the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device [*See e.g., specification, page 18, lines 19-26*].

37. A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number wherein the first sequence number comprises information on a first trusted time embedded in the storage device [*See, e.g., specification, page 18, lines 1-3*]; and

a processing device performing the following:

receives a second sequence number from the further portable device number wherein the second sequence number comprises information on a second trusted time embedded in the further portable device [*See, e.g., specification, page 18, lines 1-3*],

compares the first sequence number to the second sequence number, the first sequence number being indicative of a the first trusted time provided on the portable device, the second sequence number being indicative of the second trusted time provided on the further portable device [*See, e.g., specification, page 18, lines 1-3 and lines 10-18*], and

executes one of the following actions:

if the first trusted time is older than the second trusted time, sets the first sequence number to have a value of the second sequence number [*See e.g., specification, page 18, lines 19-26*]; and conversely,

if the second trusted time is older than the first trusted time, sets the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable

devices is mutually replaced with the newer trusted time information embedded on the other portable device [*See e.g., specification, page 18, lines 19-26*].

41. A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices [*See e.g., Figure 2, specification, page 18, lines 1-3*] the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of a the first trusted time provided on the first portable device, the second sequence number being indicative of a the second trusted time provided on the second portable device[*See e.g., specification, page 19, lines 4-10*];

if the second trusted time is newer than the first trusted time, performing a verification using at least one of the first and second keys[*See, e.g., specification, page 19, lines 10-11*];; and

setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely[*See e.g., specification, page 18, lines 19-26, page 19, lines 20-25*];,

if the first trusted time is newer than the second trusted time, performing a verification using at least one of the first and second keys[*See, e.g., specification, page 19, lines 10-11*]; and

setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device[*See e.g., specification, page 18, lines 19-26, page 19, lines 20-25*].

54. A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device[*See e.g., Figure 2, specification, page 18, lines 1-3*]; and

a processing device performing the following:

receives a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the further portable device [*See, e.g., specification, page 18, lines 1-3*],

compares the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the portable device[*See e.g., specification, page 19, lines 4-10*], the second sequence number being indicative of the second trusted time provided on the further portable device,

if the second trusted time is newer than the first trusted time, performs a verification using the first and second keys, and sets the first sequence number to have a value of the second sequence number if the verification succeeds[*See e.g., specification, page 18, lines 19-26, page 19, lines 10-11 and lines 20-25*]; and conversely,

if the first trusted time is newer than the second trusted time, performs a verification using the first and second keys, and sets the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device[*See e.g., specification, page 18, lines 19-26, page 19, lines 10-11 and lines 20-25*].

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

The rejection of claims 25-44 and 46-58 under 35 U.S.C. § 102(b) as being anticipated by Ishiguro et al. U.S. Patent No. 5,502,765 (“Ishiguro”).

The rejection of claim 45 under 35 U.S.C. § 103(a) as being obvious over Ishiguro in view of Carlisle et al. U.S. Patent No. 5,649,118 (“Carlisle”).

VII. ARGUMENT

A. **The 35 U.S.C. § 112 First Paragraph Rejection Of Claims 25-58 Should Be Reversed.**

The Final Office Action mistakenly states that there is no support for the claimed limitation “so that the older trusted time information embedded on [either] one of the two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device”. (See Office Action dated February 22, 2007, page 3).

In the previous Reply, Appellants have noted support for the claimed limitation at specification page 18 lines 26. In particular, the cited portion of the specification reads:

“If the second sequence numbers of the first and second cards 300, 350 are not equal, in step 420, it is determined (by the first card 300 and/or the second card 350) if the second sequence number SEQ2b of the second card 350 is older than the second sequence number SEQ1b of the first card 300, i.e., the time of the second card 350 is older than the time of the first card 300. If so, the [OLDER] second sequence number SEQ2b of the second card 350 is set to have the [NEWER] value of the second sequence number SEQ1b of the first card 300 (step 430). Otherwise, [i.e. conversely, if the second sequence number SEQ2b of the second card 350 is newer than the second sequence number SEQ1b of the first card 300] the [OLDER] second sequence number SEQ1b of the first card 300 is set to have the value of the [NEWER] second sequence number SEQ2b of the second card 350 (step 440).”
(underlining and parenthetical comments added for emphasis).
(See also specification FIG. 4)

Appellants submit that this portion of the text is readily understood by a person skilled in the art as an exchange or replacement of the older time on either card with the newer time on the other card. At least this portion of the specification provides explicit written support for the claimed limitation “so that the older trusted time information embedded on one of two portable

devices is mutually replaced with the newer trusted time information embedded on the other portable device.”

B. The 35 U.S.C. § 102(b) Rejections Based On Ishiguro Should Be Reversed

The Final Office Action rejects claims 25-44 and 46-58 under 35 U.S.C. § 102(b) as being anticipated by Ishiguro. The anticipation rejection is incorrect and should be reversed.

1. Relevant Case Law

To establish an anticipation rejection, the cited reference must teach every element of the claimed invention. 35 U.S.C. § 102(b) states, in pertinent part, that “[a] person shall be entitled to a patent unless “the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States.” A patent claim is anticipated under Section 102 if, among other things, “identity of invention” is shown. *Minnesota Mining and Manufacturing Co. v. Johnson & Johnson Orthopedics, Inc.*, 976 F.2d 1559, 1565, 24 U.S.P.Q.2d 1321 (Fed. Cir. 1985). In finding identity of invention, one “must show that each element of the claim in issue is found . . . in a single prior art reference.” *Id.* The Federal Circuit has held that, “[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987). Moreover, “[a] prior art publication cannot be modified by the knowledge of those skilled in the art for purposes of anticipation.” *In re Saunders*, F.2d 599, 602-03, 170 U.S.P.Q. 213, 444 (C.C.P.A. 1971). “The identical invention must be shown in as complete detail as is contained in the ... claim.” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The elements must be arranged as required by the claim. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

2. Ishiguro Does Not Disclose “If The Second [First] Sequence Number Is Newer . . . Setting The First [Second] Sequence Number To Have A Value Of The Second [First] Sequence Number . . . So That The Older Trusted Time Information Embedded On One Of Two Portable Devices Is Mutually Replaced With The Newer Trusted Time Information Embedded On The Other Portable Device”

Applicants’ claim 25 relates to a portable device capable of performing a transaction with a further portable device. The first and second portable devices have embedded thereon first and second sequence numbers comprising information on a first and a second trusted time, respectively. The system of claim 25 includes a processing device performing the steps of:

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

. . .;

if the second sequence number is newer . . . setting the first sequence number to have a value of the second sequence number . . .; and conversely,

if the first sequence number is newer . . . setting the second sequence number to have a value of the first sequence number . . .

so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

Ishiguro does not describe or teach any such two-way mutual updating of the older time with the newer time information.

The Final Office Action mistakenly cites Ishiguro col. 16 line 11 to col. 17 line 16 as describing the combination of the “if-then” steps performed by the processing device of claim

25. (See Office Action pages 5-6). Appellants note that careful reading of the cited portion does reveal any teaching of “if the second sequence number is newer . . . setting the first sequence number to have a value of the second sequence number . . .; and conversely,

if the first sequence number is newer . . . setting the second sequence number to have a value of the first sequence number . . .”.

Appellants submit that any teaching of updating time in Ishiguro is at most one-way (i.e., host to device). Ishiguro does not show or teach the two-way mutual updating of trusted information between two portable devices as described in claim 25.

Further, the Final Office Action mistakenly asserts that Ishiguro col. 15 lines 16-53 teaches “so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.” (Office Action, page 2). Appellants note that the cited portion at most teaches “the time stamp . . . set in respective IC card terminal 2 is independently updated.” (Ishiguro, col. 15, lines 40-42). There is no teaching of “mutual” updating between two portable devices.

Thus, Ishiguro does not show or teach the pair of “if-then” elements and the “so that” performed by the processing device of claim 25. For at least this reason, Ishiguro does not anticipate claim 25. Therefore, the rejection of claim 25 (and dependent claims) under 35 U.S.C. § 102(b) should be reversed.

Appellants’ claims 32, 37, 41, and 54 include the same or similar “if-then” and so that” limitations of claim 1 discussed above. The arguments relating to claim 1, set out above, are equally applicable to claims 32, 37, 41, and 54, and thus the rejection of claims 32, 37, 41, and 54 (and their dependent claims) under 35 U.S.C. § 102 should likewise be reversed.

C. The 35 U.S.C. § 103(a) Rejections Based On Ishiguro in view of

Carlisle Should Be Reversed

1. Relevant Case Law

To reject claims in an application under Section 103, an examiner must establish a *prima facie* case of obviousness. Using the Supreme Court's guidelines enunciated in *Graham v. John Deere*, 383 U.S. 1, 17 (1966), one determines "obviousness" as follows:

Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.

In *KSR Int'l Co. v. Teleflex Inc.*, (550 U.S. 398, 2007), the Supreme Court reaffirmed the *Graham* test, and indicated that although it should not be rigidly applied, a useful test for determining obviousness is to consider whether there is a teaching, suggestion or motivation in the prior art that would lead one of ordinary skill in the art to combine known elements of the prior art to arrive at the claimed invention. Importantly, the Court emphasized that a patent examiner's analysis under Section 103 should be made explicit in order to facilitate review.

Thus, to establish a *prima facie* case of obviousness, the Examiner has an obligation to construe the scope of the prior art, identify the differences between the claims and the prior art, and determine the level of skill in the pertinent art at the time of the invention. The Examiner must then provide: (1) an explicit, cogent reason based on the foregoing why it would be obvious to modify the prior art to arrive at the claimed invention; (2) a reasonable expectation of success; and (3) a teaching or suggestion of all claimed features. See M.P.E.P. §§ 706.02(j) and 2143.

2. Ishiguro Does Not Disclose "If The Second [First] Sequence Number Is Newer . . . Setting The First [Second] Sequence Number To Have A Value Of The Second [First] Sequence Number . . . So That The Older Trusted Time Information Embedded On One Of Two Portable Devices Is Mutually Replaced With The Newer Trusted Time Information Embedded On The Other Portable Device" and Carlisle fails to overcome this

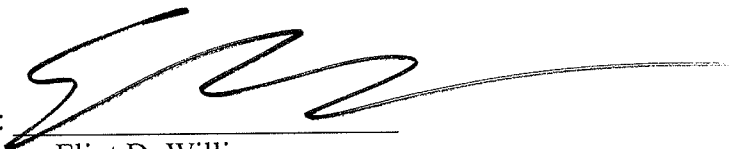
deficiency of Ishiguro.

The Examiner acknowledges that Ishiguro does not disclose or suggest “that the first and second global signing keys include a private key and a public key, wherein the verification is performed using the respective public keys, as featured in independent claim 45, but alleges that Carlisle teaches this feature of the claim and that it would be obvious to incorporate what is described in Carlisle into Ishiguro. Assuming, *arguendo*, that Carlisle describes the features alleged by the Examiner, Carlisle still fails to overcome the deficiencies of Ishiguro with respect to independent claim 41, from which claim 45 depends. Thus the rejection of claim 45 under 35 U.S.C. § 103(a) should be reversed.

D. Conclusion

For the foregoing reasons, the Examiner’s rejection of claims 25-58 should be reversed. Any fees can be charged to our Deposit Account No. 02-4377.

Respectfully submitted,

By: 

Eliot D. Williams
Patent Office Reg. No. 50,822

Telephone: (212) 408-2563

Attorneys for Appellants
Baker Botts L.L.P.
30 Rockefeller Plaza
New York, NY 10112

VIII. CLAIMS APPENDIX

The following claims are the subject of this appeal:

Claims 1-24. (Cancelled)

25. (Previously Presented) A portable device which is capable of performing a transaction with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and

a processing device performing the following steps:

receiving a second sequence number and a second key from the further portable device, wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

comparing the first sequence number to the second sequence number including comparing the embedded first and second trusted times;

performing a verification using the first and second keys;

if the second sequence number is newer than the first sequence number by comparison of the respective embedded first and second trusted times, setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first sequence number is newer than the second sequence number by comparison of the respective embedded first and second trusted times, setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

26. (Original) The portable device according to claim 25, wherein, if the verification fails, the processing device suspends the transaction with the further portable device, and records a failure of the verification.

27. (Original) The portable device according to claim 25, wherein, if the first sequence number and the second sequence number are equal, the processing device performs the transaction with the further portable device.

28. (Original) The portable device according to claim 25, wherein the storage device stores a third sequence number thereon, and wherein the processing device performs the following:
if the first sequence number and the second sequence number are equal, and
determines whether the third sequence number corresponds to a fourth sequence number of the further portable device.

29. (Original) The portable device according to claim 28, wherein, if the third sequence number corresponds to the fourth sequence number, the processing device performs the transaction with the further portable device.

30. (Original) The portable device according to claim 25, wherein the portable device is a smart card, and wherein the further portable device is a further smart card.

31. (Original) The portable device according to claim 25, wherein the first key is a global signing key, and wherein the second key is a second global signing key.

32. (Previously Presented) A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number, the second storage device storing thereon a second sequence number, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of a the first trusted time provided on the first portable

device, the second sequence number being indicative of a the second trusted time provided on the second portable device; and

if the first trusted time is older than the second trusted time, setting the first sequence number to have a value of the second sequence number and conversely,

if the second trusted time is older than the first trusted time, setting the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

33. (Original) The method according to claim 32, further comprising the step of:

if the second time is older than the first time, setting the second sequence number to have a value of the first sequence number.

34. (Original) The method according to claim 33, further comprising the step of:

after the setting step and if the first time is not equal to the second time, executing an action which is triggered by at least one of the first sequence number and the second sequence number.

35. (Original) The method according to claim 34, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the executing step and if the first time is not equal to the second time, performing a transaction between the first card and the second card.

36. (Original) The method according to claim 32, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the first time is equal to the second time, performing a transaction between the first card and the second card.

37. (Previously Presented) A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and
a processing device performing the following:

receives a second sequence number from the further portable device number wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,
compares the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the portable device, the second sequence number being indicative of the second trusted time provided on the further portable device, and
executes one of the following actions:

if the first trusted time is older than the second trusted time, sets the first sequence number to have a value of the second sequence number; and
conversely,

if the second trusted time is older than the first trusted time, sets the second sequence number to have a value of the first sequence number so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

38. (Original) The portable device according to claim 37, wherein, if the first time is not equal to the second time, the processing device executes a particular action which is triggered by at least one of the first sequence number and the second sequence number.

39. (Original) The portable device according to claim 37,
wherein the portable device is a smart card, and the further portable device is a further smart card, and

wherein, after the execution of the particular action and if the first time is not equal to the second time, the processing device performs a transaction between the smart card and the further smart card.

40. (Original) The portable device according to claim 37,
 wherein the portable device is a smart card, and the further portable device is a further smart card, and
 wherein, if the first time is equal to the second time, the processing device performs a transaction between the smart card and the further smart card.

41. (Previously Presented) A method for determining an approximate current time using a first portable device and a second portable device, the first portable device having a first storage device, the second portable device having a second storage device, the first storage device storing thereon a first sequence number and a first key, the second storage device storing thereon a second sequence number and a second key, wherein the first and second sequence numbers comprise information on a first and a second trusted time embedded in the respective storage devices, the method comprising the steps of:

comparing the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the first portable device, the second sequence number being indicative of the second trusted time provided on the second portable device;

if the second trusted time is newer than the first trusted time, performing a verification using at least one of the first and second keys; and

setting the first sequence number to have a value of the second sequence number if the verification succeeds; and conversely,

if the first trusted time is newer than the second trusted time, performing a verification using at least one of the first and second keys; and

setting the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

42. (Original) The method according to claim 41, further comprising the steps of:

generating the cryptograms by one of the first portable device and the second portable device; and

verifying the cryptograms using another one of the first portable device and the second portable device.

43. (Original) The method according to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the verification is performed by comparing at least one first portion of the first global signing key to at least one second portion of the second global signing key.

44. (Original) The method according to claim 43, wherein the verification succeeds when the at least one first portion corresponds to the at least one second portion.

45. (Original) The method according to claim 43, wherein each of the first and second global signing keys includes a private key and a public key, and wherein the verification is performed using the respective public keys.

46. (Original) The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

after the setting step, performing a transaction between the first card and the second card.

47. (Original) The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the verification fails, suspending a transaction between the first card and the second card.

48. (Original) The method according to claim 41, further comprising the step of:

if the verification fails, recording a failure of the verification in at least one of the first storage device and the second storage device.

49. (Original) The method according to claim 41, wherein the first portable device is a first card, and the second portable device is a second card, and further comprising the step of:

if the first time and the second time are equal, performing a transaction between the first card and the second card.

50. (Original) The method according to claim 41, wherein the first portable device is a first card and the second portable device is a second card,

wherein the setting step is performed by transmitting an authenticated system message command from the second card to the first card, and

wherein at least one of the first and second cards sets the second sequence number.

51. (Original) The method according to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the first global signing key relates to the first sequence number, and the second global signing key relates to the second sequence number.

52. (Original) The method according to claim 41, wherein the first key is a first global signing key, and the second key is a global signing key, and wherein the first global signing key is associated with a first value transfer protocol ("VTP") key, and the second global signing key is associated with a second VTP key, the first VTP key being stored in the first storage device, the second VTP key being stored in the second storage device.

53. (Original) The method according to claim 41, wherein each of the first portable device and the second portable device includes a processing device.

54. (Previously Presented) A portable device which is capable of determining an approximate current time during a communication with a further portable device, comprising:

a storage device storing a first sequence number and a first key wherein the first sequence number comprises information on a first trusted time embedded in the storage device; and
a processing device performing the following:

receives a second sequence number and a second key from the further portable device wherein the second sequence number comprises information on a second trusted time embedded in the further portable device,

compares the first sequence number to the second sequence number, the first sequence number being indicative of the first trusted time provided on the portable device, the second sequence number being indicative of the second trusted time provided on the further portable device,

if the second trusted time is newer than the first trusted time, performs a verification using the first and second keys, and sets the first sequence number to have a value of the second sequence number if the verification succeeds; and
conversely,

if the first trusted time is newer than the second trusted time, performs a verification using the first and second keys, and sets the second sequence number to have a value of the first sequence number if the verification succeeds so that the older trusted time information embedded on one of two portable devices is mutually replaced with the newer trusted time information embedded on the other portable device.

55. (Original) The portable device according to claim 54, wherein, if the verification fails, the processing device suspends the transaction with the further portable device, and records a failure of the verification.

56. (Original) The portable device according to claim 54, wherein, if the first sequence number and the second sequence number are equal, the processing device performs the transaction with the further portable device.

57. (Original) The portable device according to claim 54, wherein the portable device is a smart card, and wherein the further portable device is a further smart card.

58. (Original) The portable device according to claim 54, wherein the first key is a first global signing key and the second key is a second global signing key.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.